КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

26 апреля 2018 г.
г. Санкт-Петербург

#CODEIB

ПОДХОД McAfee К ПОСТРОЕНИЮ АДАПТИВНОЙ ЗАЩИТЫ

ИВАН ОЖЕРЕЛЬЕВ,
КОМПАНИЯ MONT

ТЕЛЕФОН: +7 (985) 802-34-39
EMAIL: IOZHERELIEV@MONT.COM

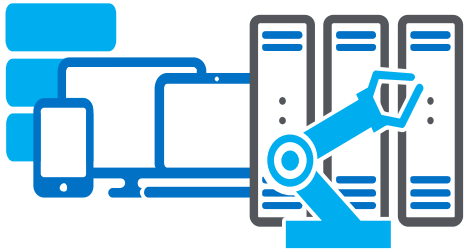
McAfee™
Together is power.

Фундаментальные изменения в нашем цифровом мире

Пользователи

Мобильные | Удаленные| Корпоративные

Растущее количество устройств и данных



Миллиард устройств
Зеттабайт Данных
Интернет вещей

Облако

Частные / Публичные гибридные

Собственные устройства

BYOD
Теневая IT
Ориентир на пользователей

Организации должны внедрять инновации, работать, и расти с уверенностью

Cybercrime cost the global economy $600 billion in 2017.

McAfee

Together is powe

McAfee

- 462+ миллиона рабочих станций
- 97,910+ заказчиков
- 7,108+ сотрудников
- 190+ стран
- 137+ Innovation Alliance партнеров
- 1,300+ патентов по безопасности

Решения McAfee

На рынке РФ

Сколько

Cloud Security

Endpoint protection

SIEM

Более 20…

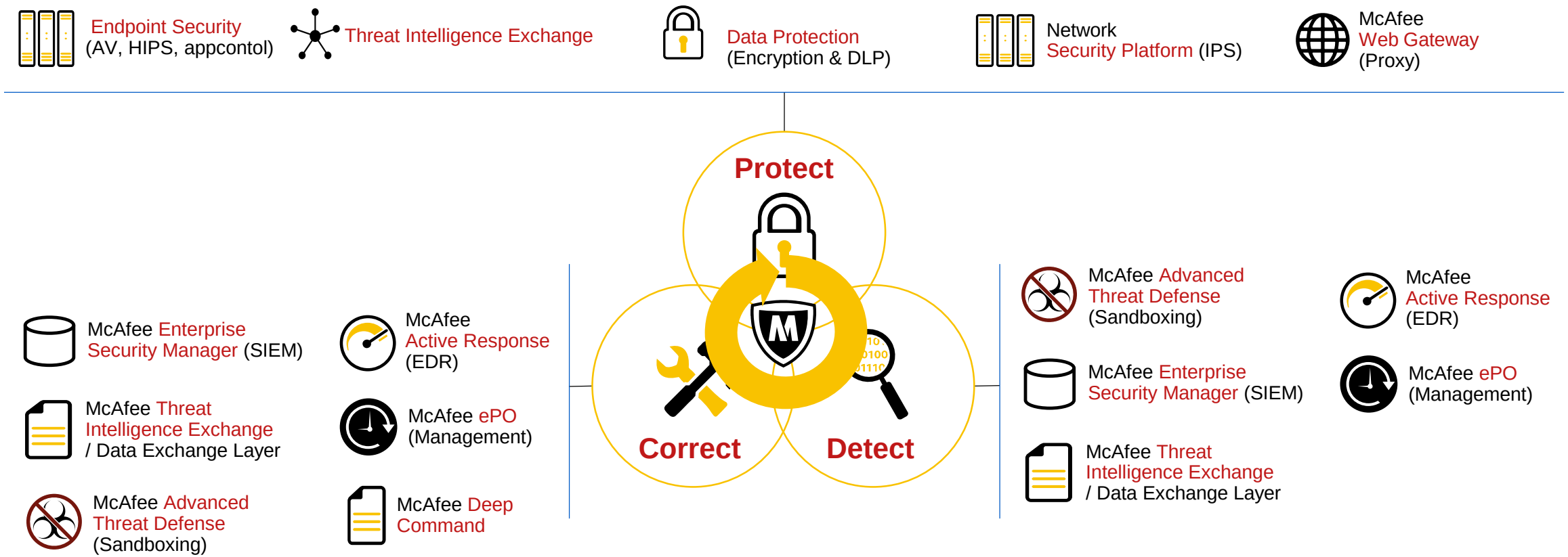
Data protection

Security management

Network security

Content security

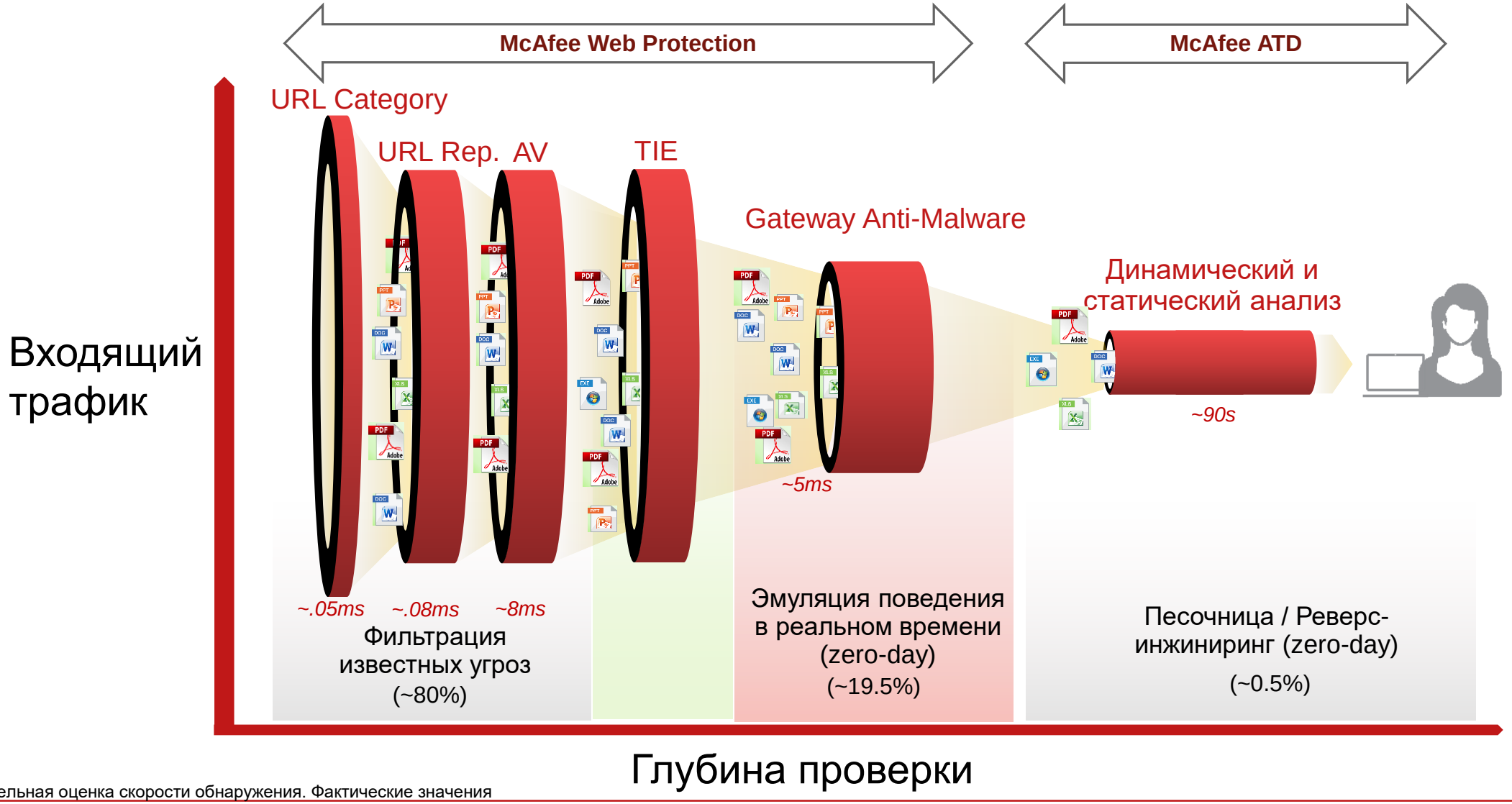
Взаимосвязанная инфраструктура



McAfee Web Gateway

Обнаружение угроз в веб-трафике

Фильтрация известных угроз и zero-day в реальном времени, оставшиеся подозрительные отправляются в ATD

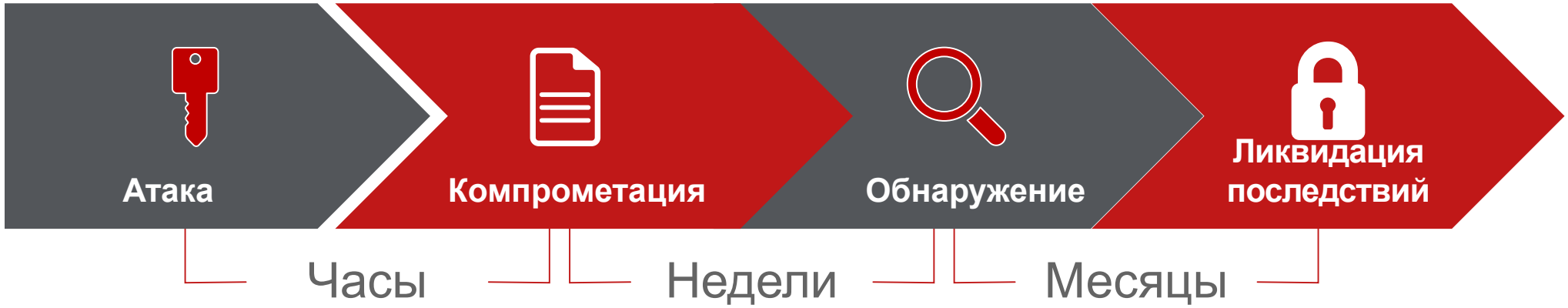


Приблизительная оценка скорости обнаружения. Фактические значения могут отличаться.

SIEM

Задача

Обнаружить угрозу и устранить последствия



Время на противодействие атаке

46 DAYS[1]

Средняя стоимость в день

$21,155[1]

The average cost of a data breach involving fewer than 10,000 records was $5 million[1]

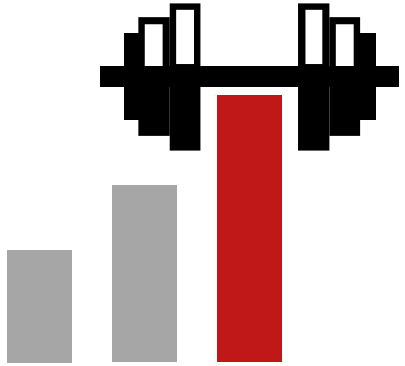
[1]Ponemon Institute 2016 Cost of Cyber Crime Study: United States study

McAfee Threat Intelligence Exchange

Подход Threat Intelligence Exchange

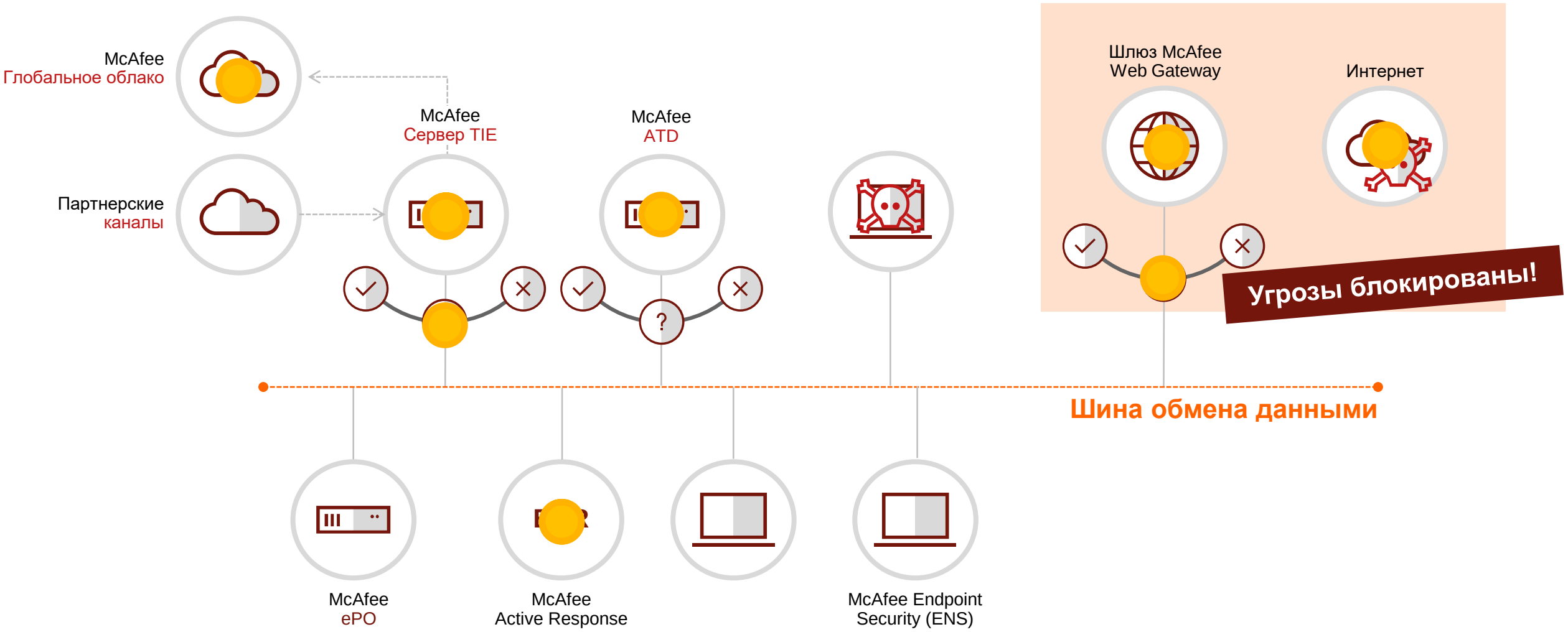
ИБ решения должны функционировать совместно

ИБ решения должны обмениваться опытом



ИБ решения должны непрерывно становиться сильнее

Обзор решения TIE



Open Data Exchange Layer

Интеграция решений до DXL

Для начала интеграция
двух решений

Интеграция решений до DXL

Сначала обмен базовой информацией, host names, credentials, чтобы решения могли начать обмен данными

Решение #2

Решение #1

Credentials

X Обмен учётными данными

Интеграция решений до DXL

Каждый продукт
интегрируется с каждым
с использованием
специализированного

Решение #2

Решение #1

Credentials

API

X	Обмен учётными данными
X	Интеграция на уровне API

Интеграция решений до DXL

Необходимо отрегулировать сетевые политики для разрешения сетевого обмена между решениями (ports, protocols)

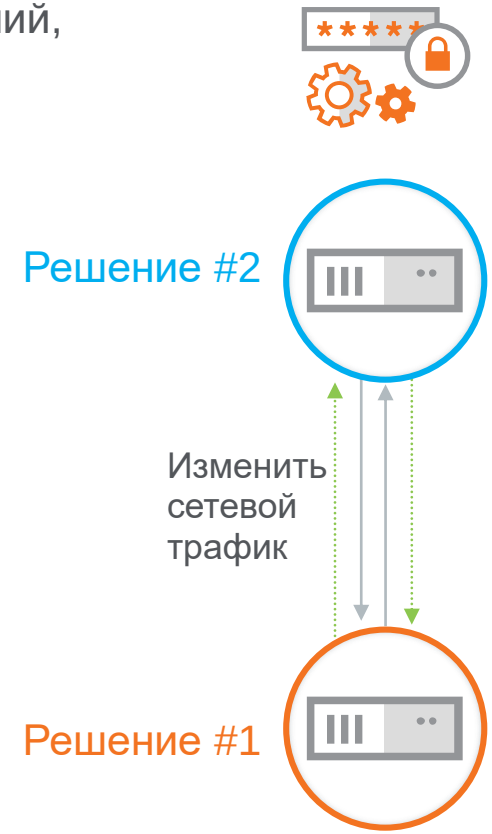
X	Обмен учётными данными
X	Интеграция на уровне API
X	Регулирование сети для портов и протоколов

Credentials

API

Интеграция решений до DXL

Для получения изменений, решения регулярно опрашивают друг друга



X	Обмен учётными данными
X	Интеграция на уровне API
X	Регулирование сети для портов и протоколов
X	Опрос изменение (simulate real-time events)

Credentials

API

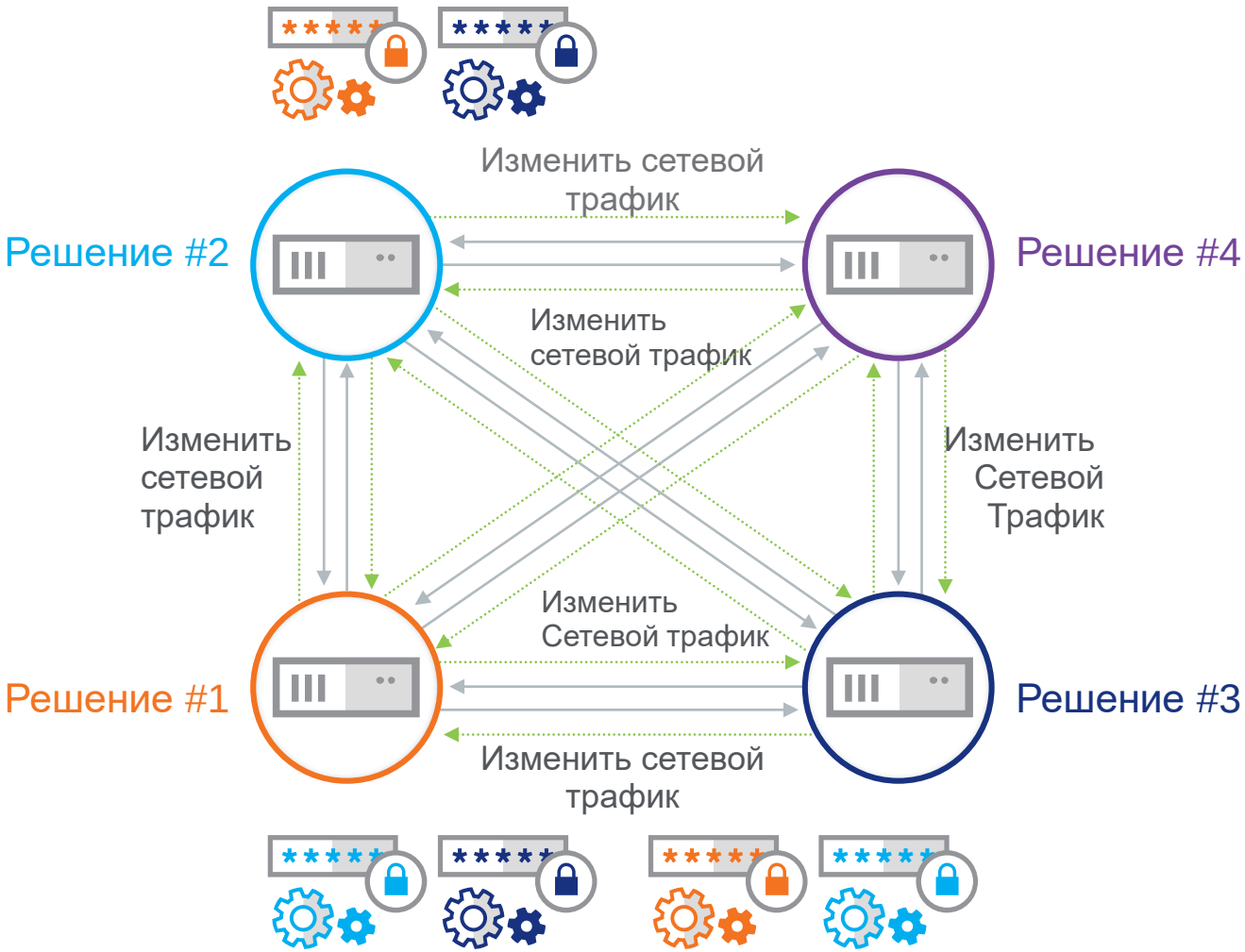
Интеграция решений до DXL

Сложность взаимодействий увеличивается с каждым новым решением

X	Обмен учётными данными
X	Интеграция на уровне API
X	Регулирование сети для портов и протоколов
X	Опрос изменение (simulate real-time events)

Интеграция решений до DXL

По-моему этим
очень сложно управлять



X	Обмен учётными данными
X	Интеграция на уровне API
X	Регулирование сети для портов и протоколов
X	Опрос изменение (simulate real-time events)

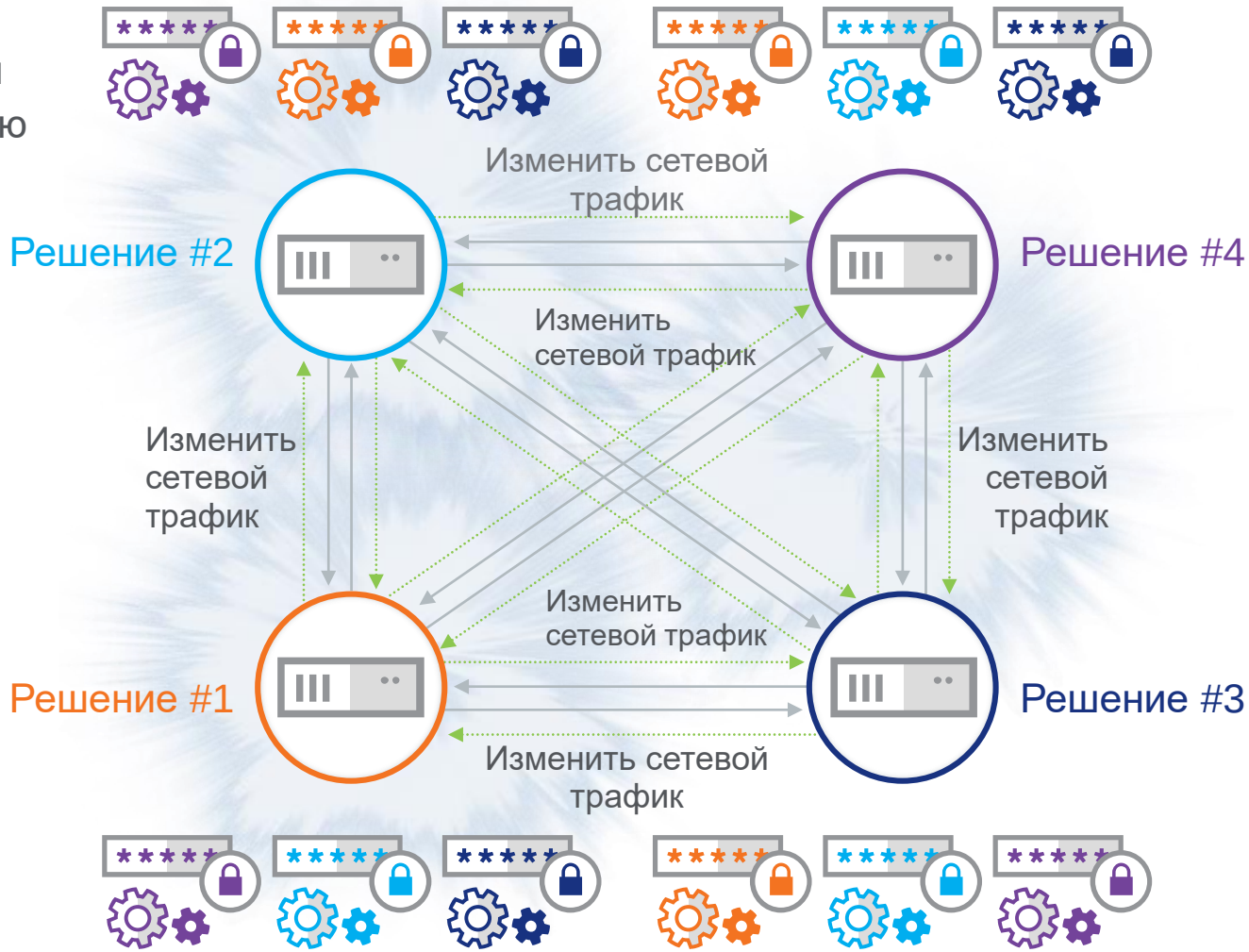
Credentials

API

Интеграция решений до DXL

Затрачено очень много времени и усилий чтобы построить такую сложную систему из нескольких решений.

Когда в одном из продуктов изменитсяAPI (что бывает), всё сломалось начинаем сначала!



X	Обмен учётными данными
X	Интеграция на уровне API
X	Регулирование сети для портов и протоколов
X	Опрос изменение (simulate real-time events)

Credentials

API

Партнёры Security Innovation Alliance

SIA Partners

Current as of 7/21/2017

Connected Today

- Advanced Cyber Security
- aruba, a Hewlett Packard Enterprise company — POC
- Avecto
- boldonjames, A CimetIQ Company
- Check Point Software Technologies Ltd.
- CICADA Security Technology
- FORCEPOINT
- HUAWEI — POC
- RAPID7
- TITUS
- TYCHON
- TRAPX SECURITY

In Testing or Development Today

- Attivo Networks
- Autonomic Software
- Guidance Software
- GURUCUL
- Infoblox — Control Your Network
- INTERSET
- Lumeta
- MobileIron
- NIKSUN
- proofpoint
- THREATCONNECT

In Design

- ayehu
- BeyondTrust — Visibility. Knowledge. Action.
- BUFFERZONE
- CISCO
- CYPHORT
- DFLABS — Cyber Incidents Under Control
- Extreme — Connect Beyond the Network
- ForeScout
- JUNIPER NETWORKS
- Phantom
- sas
- tenable network security
- vmware airwatch
- THALES

Вопросы?

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

26 апреля 2018 г.
г. Санкт-Петербург

#CODEIB

КОТ ИБ

ИВАН ОЖЕРЕЛЬЕВ,
КОМПАНИЯ MONT

ТЕЛЕФОН: +7 (985) 802-34-39
EMAIL: IOZHERELIEV@MONT.COM